Indiana INVESTIGATES

A MAGAZINE FOR INDIANA AUDITORS AND INVESTIGATORS

VOLUME 2, ISSUE 3
SEPTEMBER 2007

In this issue:

A Publication by:
The Office of Inspector General
Melissa Nees Hauger, Editor
150 West Market Street, Room 414
Indianapolis, IN 46204
317.232.3850

2007 Meetings

Indiana Auditors and Investigators
Quarterly Meetings:

Thursday, September 20, 9:00-10:30
IGCS Conf. Rm. 17
Annual Summit, December 2007
Date, location TBA

Did you know...

"According to the FBI, cybercrime costs businesses and the government more than $10 billion a year, with computer-aided identity theft costing an additional $1 billion a year. The FBI also estimates that more than 80% of computer crime goes unreported, often because businesses think law enforcement agencies lack the resources and skills to combat it."
Medaris, Kim. "Deciphering Digital Evidence." *Innovation* Spring 2007: 10-13.

Does your agency have news or ideas to share? We would love to hear from you. Please email Melissa Hauger at mhauger@ig.in.gov.

MEETING SUMMARY

June 21, 2007

At our June meeting, Superintendent Alex Huskey and Officer Tony McGail of the Indiana State Excise Police gave an informative presentation on their agency. The Indiana State Excise Police are the law enforcement division of the Alcohol and Tobacco Commission. State Excise police officers are empowered by statute to enforce the laws and rules of the Alcohol and Tobacco Commission as well as the laws of the State of Indiana. The agency's primary goal is to reduce the access and availability of alcohol and tobacco products to minors.

The Excise Police assist the Alcohol and Tobacoo Commission (ATC) with regulating nearly 10,000 permits for the manufacturing, operation, or sale of alcoholic beverages at all restaurants, breweries, wineries, grocery stores, hotels, drug stores, package stores, stadiums, civic centers, social and fraternal clubs, horse tracks and river boats throughout the State of Indiana. In addition, the ATC and Excise Police also license and regulate the permits of every bartender, waiter, waitress, salesperson and clerk associated with the sale or service of alcoholic beverages in the State of Indiana, almost 100,000 in number. They have raised a revenue of approximately $42 million for the citizens of Indiana.

The Excise Police consist of 89 officers in six district offices across the state. All officers are sworn-in police officers with full law enforcement powers. They receive tips and complaints from employees (often recently terminated), parents, restaurant patrons, other agencies (i.e. Department of Health), and other law enforcement agencies (often in cases of DUI or drugs). Once they receive the alleged information, they often inspect the alleged business/location in violation. They look for things such as changes in floor plans, location, and change of ownership, and then proceed to investigate. Common offenses include sales to a minor, public intoxication, sale/use of tobacco products to a minor, or false identification.

The Excise Police are committed to professional law enforcement development and training, as well as partnerships with other state, local, and federal agencies. They have developed various programs such as Cops in Shops, where excise officers pose as employees or customers at dealer establishments and can arrest minors purchasing alcohol. Other programs include ICE (Intensified College Enforcement), SUDS (Stop Underage Drinking and Sales), and TRIP (Tobacco Retailer Inspection Program), which establishes progressive penalties for retailers and clerks who sell tobacco to anyone under the age of 18.

In addition to the presentation given by the Excise Police, the group briefly discussed ways to certify our training at our quarterly meetings. Inspector General David Thomas also gave a brief training on the Indiana Code of Ethics.

State Excise Police Officers arrest a young man guilty of producing false ids. Photo: Jeremy Hogan - Herald Times

WORKPLACE SECURITY

Keeping Employees Honest

By David Johnston, Enforcement Analyst, National White Collar Crime Center (NW3C)

Recently companies have begun to shift their focus from physical security to operational security. The shift is not to discredit the importance of physical security, as it still plays an important role in the workplace. Rather, companies are beginning to understand the threats that are posed within their own walls. Physical security only serves to keep the undesired out. Operational security goes the extra step and attempts to keep insiders honest.

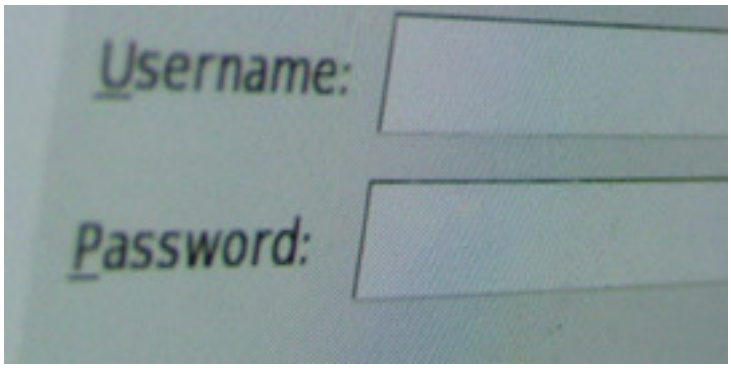
Although different in nature, physical security and operational security possess some similarities, the most common being their goals of deterrence and detection. Of course, their methods differ in the ways they achieve these goals. For example, a company may install an alarm system on the doors as a form of physical security. Unauthorized persons trying to seek entry will either be deterred knowing the chances of being caught are greater at this company than at one without an alarm system, or they will attempt to break in and be detected when the alarm sounds.

The same company may also implement a system of checks and balances as a form of operational security. An employee may choose to be honest because he or she knows that there is a better chance of being caught when others are watching. If that employee chooses to be dishonest, chances are he or she will be caught soon thereafter. Two different methods of security, yet both yield the same outcomes: deterrence and detection. Evaluating what types of security a company needs can be a difficult task. Companies need to first figure out what needs to be protected, and then try to determine the best way to protect those items within their budgets.

The interesting part about operational security is that there are no limits. Physical security eventually has limits. You can install just so many alarms, keypads, passwords, and biometric scanning devices before you have exhausted all options. Operational security, on the other hand, allows companies the flexibility to use their resources in many ways; it is virtually open-ended. Because there are so many options when it comes to operational security, it is worthwhile to take a closer look at it, beginning with typical threats and then moving on to some common ways to detect and deter those threats.

Evaluating the Risks

The most common risks presented to companies of all sizes are embezzlement, asset theft, purchasing fraud, and falsified accounting records. This list does not exhaust all risk factors, but focuses on those that most greatly affect all businesses today. Embezzlement is among the top concerns of businesses today. It is estimated that nearly one-third of all employees will steal from their place of



employment, totaling millions of dollars lost per annum. Additionally, it is estimated that twice as many people will steal if the chances of being caught are slim. If that were to happen, the losses would be crippling to companies. The point is that you have to make certain that employees know that theft will not go unnoticed.

The only way to know what you are missing is to know what you have, or are supposed to have. That is why it is best to have someone assigned to audit what the company has on hand.

What you are probably thinking now is: what happens if the auditor is among the one third who will steal from the company? Major business activities (transactions, asset control, etc.) should never have just one employee assigned to those tasks. A system of checks needs to be established. This accounts for the off chance that a

dishonest employee has been assigned to a major task. In such a case where a dishonest employee is in a position where they can take advantage of the company, a second employee will be assigned to "check" their work to make sure it is done properly. It is important to remember that such a policy should be adopted for all activities so that its implementation does not imply guilt on any employee.

Aside from embezzlement, which refers mostly to the theft of money, a company must also be concerned with the theft of its physical assets. A physical asset refers mostly to inventory. Inventory consists of items that can be sold for profit, or items that were purchased and hold value for the company (computers, office supplies, etc.). Similar to embezzlement, the best way to prevent this loss is to know what you have on hand. Assign a couple of employees to take count of inventory, making note of who is in possession of certain items. A good example of this would be a company that issues laptops to its employees. When a laptop is issued, make note of who it goes to. This way, if the laptop comes up missing, you know who to turn to for answers.

For companies with large supply rooms, it may be a good idea to set up surveillance cameras to capture what occurs in the inventory room. If surveillance is conducted, make sure to notify all employees of the cameras so that nobody feels as though their privacy has been violated. Another risk can be associated with a company's purchases. Purchasing fraud occurs when a purchasing manager makes a connection with a specific supplier. The two parties enter into an agreement that all products will be purchased through this particular supplier, who turns out to be a friend of sorts. This friend overcharges for the products sold and pockets the difference, giving a cut of the money to the purchasing manager as an incentive for doing business.

The best way to prevent this is to have several employees look into various vendors that offer the same supplies. Once a fair price for goods is established, it will become evident if the company is overpaying for goods. The investigation can establish itself from this point.

Falsified accounting records are probably one of the biggest threats to a corporation. This is due to the fact that there are so many ways to perpetrate this scheme. Some of the common ways to initiate this scheme are hiding or forging receipts, stealing petty cash, and creating fictitious employees for payroll.

Forging a receipt occurs when a receipt is recorded at a lower amount than what the customer paid. This allows the perpetrator to pocket the difference between the actual amount and the recorded amount. On the books everything looks kosher; the company receives the amount that the receipt shows was due. However, unbeknownst to the company, the receipt is incorrect.

The biggest clue of a forged receipt is a photocopied receipt. A photocopy can hide any alterations that would have been made on the original amount. Anytime a photocopied receipt is found, it is wise to inquire about the original receipt and its whereabouts.

Hiding a receipt takes this scheme to the next level. Instead of altering the receipt to show a lower amount, the receipt just does not appear. As a result, the company does not expect to see money for anything, and therefore the perpetrator can pocket the full amount of the purchase.

Hidden receipts can be uncovered by counting inventory and knowing the company's operational capacity. If a company has five hundred products to sell at ten dollars

per item, they should show a profit of five thousand dollars when the entire inventory has been sold off. If the entire inventory is gone, but the company is only showing a profit of three thousand dollars, then two conclusions can be drawn. Either inventory sales have not been recorded (hiding receipts), or inventory has been stolen.

Payroll fraud is another concern of some companies. A payroll manager has the ability to pay all workers. They also have the ability to create people to pay that really are not employed by the company at all. The fictitious employee that is created is actually the payroll manager, who will not only cut a check to this fictitious person, but will cash in on it as well. The check goes through the pay cycle without raising any eyebrows because it appears to be going to a legitimate employee. The problem is the payroll manager is getting paid twice without anybody knowing it.

When it comes to falsified accounting records, the best way to prevent and detect such activities is to closely monitor all transactions. Have more than one person recording receipts. That way, if one person sees something out of the ordinary taking place, they can report it. All work should be approved by someone else. Also, keep track of your operational capacity. If you do not know what you have, then you certainly will not be able to detect what you are missing.

Fraud Detection

An employee has committed a fraud, and knowing that the company has no structure in place to catch a fraud in progress, the perpetrator knows that as soon as the money is out the door he/she will never be caught. On the other hand, the company suspects they have been defrauded by an employee and figures that there is no way to determine if their hunch is true because they failed to setup a structure to catch fraud. The company gives up, and the perpetrator gets away with the crime.

In the criminal's mind, this would be the perfect world. In most cases, this is what happens, unfortunately. The truth is that a company should not give up on a fraud investigation. Although operational security was foregone, there are still options once the fraud has occurred. The key is to be discreet when investigating an individual suspected of fraud because if it turns out that a fraud did not occur, you do not want to get sued for defamation of character.

To help determine if a fraud has occurred, you need to identify some red flags. A red flag is anything that would suggest the commission of a crime. A couple of the most common red flags of employee fraud are a rise in the employee's living standards and the employee becoming a work-a-holic.

An employee who is committing fraud has more money to work with in their personal life. The extra money allows for investments and other large purchases. A lavish lifestyle that is out of the ordinary can raise questions as to where the extra money is coming from.

This red flag is sometimes termed "living beyond one's means," and refers to someone who is spending more money than he/she can justify having based on his/her income. Performing a net worth calculation is the best way to determine if someone is living beyond their means.

Calculating net worth is a five step process. The first step is separating a person's assets from their liabilities. Two totals are generated: total assets and total liabilities. The two are then subtracted from each other to determine a net worth. The next step is subtracting the previous year's net worth from the current year's net worth, leaving the change in net worth.

From there, you add in total living expenses and subtract total income. This leaves the income from concealed sources. Depending on the amount of income from concealed sources, you can determine if there is cause to believe a fraud has occurred.

Work-a-holic is a term given to people who spend the majority of their time at work. They are the type that are the first in, and the last out. They never take vacations, and even come in to work when sick. Work-a-holics live for work and never miss a day. Some companies would see this as a dedicated worker. However, it can be a cause for concern.

When an employee is at work he/she can see everything that happens, and more importantly they make

sure nobody sees what he/she is doing. A person trying to hide a fraud will not want anyone to see what he/she is doing for fear that the scheme will be uncovered. The only way to keep someone away is to show up every day all the time. Missing a day would mean that someone else would have to step in and do the job.

Be cautious of work-a-holics because, although they may seem to be dedicated workers, they may also be trying to hide something. Remember that things are not always as good as they may seem.

Fraud Prevention

The key to fraud prevention is remembering that increasing the risk over the reward will help deter employees from committing an offense. The higher the risk presented, the more honest an employee will be. However, it is not always about making and maintaining honest employees. It is about hiring honest employees.

Before an employee is hired, a thorough background check should be performed. This gives a "heads-up" of what to expect of a person before they even start. A background check allows a company to decide if a certain candidate can be trusted as an employee. If they cannot be trusted, and are not an honest candidate, it would be desirable not to hire that person. Hiring a dishonest person is opening the door to future problems.

On the administrative end, the company should establish clear operating policies. These policies let employees know what is expected of them, as well as what is not expected of them. A company should never assume that an employee knows the policies coming into the job. Setting a good tone from the top down is the most effective way to strengthen the established policies. If the executive staff does not adhere to the policies then it sets a bad example for the rest of the company, which could lead to many problems down the road.

The final and most obvious way to prevent fraud is to make it hard for an employee to commit fraud. The first way to do this is to establish positions so that two people do the same job. If there are two people doing the same job, they are constantly keeping an eye on each other's work; making it hard to commit a fraud without being caught.

To take that a step further, establish a system of checks. When work is completed, have a manager check it over. Not only is this a good way to catch mistakes, but it eliminates the opportunity for employees to conspire for the purpose of committing a fraud.

Finally, rotate positions within a company. If an employee is trying to hide something it will certainly surface when someone else steps in to do their job. A lesser form of this method would be to mandate vacation time. When an employee is out on vacation, someone else takes their spot. If something is out of order, it will certainly be caught at this point.

Although large companies are more often the victims of dishonest employees, small companies are affected more by each individual crime. The reason big companies are victims more often is because it is easier to steal a few thousand dollars from a multi-million dollar company than it is from a company that does not have nearly the same amount of assets. The reason why small companies are more greatly affected is because they do not have as many resources to recoup the losses. As a matter of fact, some companies can never recover from such financial crimes.

Published with permission from *Informant* Magazine, March - June 2007
Vol.3, No. 1